CLAIMS

What is claimed is:

1. An apparatus to hierarchically encrypt media data, comprising:

an N-th layer key generator generating an N-th layer key;

an (N+1)-th layer key generator generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;

an N-th layer data encryptor encrypting N-th layer data using the N-th layer key; and

an (N+1)-th layer data encryptor encrypting (N+1)-th layer data using the (N+1)-th layer key.

2. The apparatus of claim 1, wherein the predetermined function is a one-way function to deduce a value of the function from an input value but not to deduce the input value from the value of the function.

3. The apparatus of claim 1, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

4. The apparatus of claim 1, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

5. The apparatus of claim 4, wherein the N-th layer key generator generates the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

6. The apparatus of claim 1, further comprising:

an N-th layer key buffer temporarily storing the N-th layer key;

an N-th layer key generation commander commanding the N-th layer key generator to generate the N-th layer key according to meta-data when the meta-data is received; and

an N-th layer key supply commander commanding the N-th layer key buffer to supply the N-th layer key to the N-th layer data encryptor according to the meta data when the N-th layer data is received.

7. The apparatus of claim 1, further comprising:

an (N+1)-th layer key buffer temporarily storing the (N+1)-th layer key;

an (N+1)-th layer key generation commander commanding the (N+1)-th layer key generator to generate the (N+1)-th layer key according to meta-data when the meta-data is received; and

an (N+1)-th layer key supply commander commanding the (N+1)-th layer key buffer to supply the (N+1)-th layer key to the (N+1)-th layer data encryptor according to the meta data when the (N+1)-th layer data is received.

8. The apparatus of claim 1, further comprising:

an N-th layer key encryptor encrypting the N-th layer key.

9. The apparatus of claim 8, further comprising:

an encrypted N-th layer key transmitter transmitting the encrypted N-th layer key.

10. The apparatus of claim 8, further comprising:

an encrypted N-th layer key storage block storing the encrypted N-th layer key; and

an encrypted N-th layer key transmitter transmitting the encrypted N-th layer key stored in the encrypted N-th layer key storage block upon a request from a user.

11. The apparatus of claim 1, further comprising:

an (N+1)-th layer key encryptor encrypting the (N+1)-th layer key.

12. The apparatus of claim 11, further comprising:

an encrypted (N+1)-th layer key transmitter transmitting the encrypted (N+1)-th layer key.

13. The apparatus of claim 11, further comprising:

an encrypted (N+1)-th layer key storage block storing the encrypted (N+1)-th layer key; and

an encrypted (N+1)-th layer key transmitter transmitting the encrypted (N+1)-th layer key stored in the encrypted (N+1)-th layer key storage block upon a request from a user.

14. The apparatus of claim 1, further comprising:

an encrypted N-th layer data transmitter transmitting the encrypted N-th layer data.

15. The apparatus of claim 1, further comprising:

an encrypted N-th layer data storage block storing the encrypted N-th layer data; and

an encrypted N-th layer data transmitter transmitting the encrypted N-th layer data stored in the encrypted N-th layer data storage block upon a request from a user.

16. The apparatus of claim 1, further comprising;

an encrypted (N+1)-th layer data transmitter transmitting the encrypted (N+1)-th layer data.

17. The apparatus of claim 1, further comprising:

an encrypted (N+1)-th layer data storage block storing the encrypted (N+1)-th layer data; and

an encrypted (N+1)-th layer data transmitter transmitting the encrypted (N+1)-th layer data stored in the encrypted (N+1)-th layer data storage block upon a request from a user.

18. An apparatus to hierarchically decrypt media data, comprising:

an N-th layer key generator generating an N-th layer key;

an (N+1)-th layer key generator generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;

an encrypted N-th layer data decryptor decrypting encrypted N-th layer data using the N-th layer key; and

an encrypted (N+1)-th layer data decryptor decrypting encrypted (N+1)-th layer data using the (N+1)-th layer key.

19. The apparatus of claim 18, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

20. The apparatus of claim 18, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

21. The apparatus of claim 20, wherein the N-th layer key generator receives an N-th layer key and generates the N-th layer key.

22. The apparatus of claim 20, wherein the N-th layer key generator comprises:

an encrypted N-th layer key receiver receiving the encrypted N-th layer key; and

an encrypted N-th layer key decryptor decrypting the encrypted N-th layer key to generate the N-th layer key.

23. The apparatus of claim 18, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

24. The apparatus of claim 23, wherein the N-th layer key generator generates the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

25. The apparatus of claim 18, further comprising:

an N-th layer key buffer temporarily storing the N-th layer key;

an N-th layer key generation commander commanding the N-th layer key generator to generate the N-th layer key according to meta-data when the meta-data is received; and

an N-th layer key supply commander commanding the N-th layer key buffer to supply the N-th layer key to the encrypted N-th layer data decryptor according to the meta data when the encrypted N-th layer data is received.

26. The apparatus of claim 18, further comprising:

an (N+1)-th layer key buffer temporarily storing the (N+1)-th layer key;

an (N+1)-th layer key generation commander commanding the (N+1)-th layer key generator to generate the (N+1)-th layer key according to meta-data when the meta-data is received; and

an (N+1)-th layer key supply commander commanding the (N+1)-th layer key buffer to supply the (N+1)-th layer key to the encrypted (N+1)-th layer data decryptor according to the meta data when the encrypted (N+1)-th layer data is received.

27. An apparatus to hierarchically encrypt and decrypt media data, comprising:

a hierarchical encryption unit generating an N-th layer key, generating an (N+1)-th layer key by applying the generated N-th layer key to a predetermined function, encrypting N-th layer data using the N-th layer key, and encrypting (N+1)-th layer data using the generated (N+1)-th layer key; and

a hierarchical decryption unit generating the N-th layer key, generating the (N+1)-th layer key by applying the N-th layer key to the predetermined function, decrypting the encrypted N-th layer data using the N-th layer key, and decrypting the encrypted (N+1)-th layer data using the (N+1)-th layer key.

28. The apparatus of claim 27, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

29. The apparatus of claim 27, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

30. The apparatus of claim 27, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

31. The apparatus of claim 5, wherein the N-th layer key generator generates the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

32. A method of hierarchically encrypting media data, comprising:

generating an N-th layer key;

generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;

encrypting N-th layer data using the N-th layer key; and

encrypting (N+1)-th layer data using the (N+1)-th layer key.

33. The method of claim 32, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

34. The method of claim 33, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

35. The method of claim 32, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

36. The method of claim 35, wherein the generating of the N-th layer key comprises generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

37. The method of claim 32, further comprising:

temporarily storing the N-th layer key;

commanding that the N-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored N-th layer key be supplied to encrypt the N-th layer data according to the meta data when the N-th layer data is received.

38. The method of claim 32, further comprising:

temporarily storing the (N+1)-th layer key;

commanding that the (N+1)-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored (N+1)-th layer key be supplied to encrypt the (N+1)-th layer data according to the meta data when the (N+1)-th layer data is received.

39. The method of claim 32, further comprising:

encrypting the N-th layer key.

40. The method of claim 39, further comprising:

transmitting the encrypted N-th layer key.

41. The method of claim 39, further comprising:

storing the encrypted N-th layer key; and

transmitting the encrypted and stored N-th layer key upon a request from a user.

42. The method of claim 32, further comprising:
encrypting the (N+1)-th layer key.

43. The method of claim 42, further comprising:
transmitting the encrypted (N+1)-th layer key.

44. The method of claim 42, further comprising:
storing the encrypted (N+1)-th layer key; and
transmitting the encrypted and stored (N+1)-th layer key upon a request from a user.

45. The method of claim 32, further comprising:
transmitting the encrypted N-th layer data.

46. The method of claim 32, further comprising:
storing the encrypted N-th layer data; and
transmitting the encrypted and stored N-th layer data at a user's request.

47. The method of claim 32, further comprising:
transmitting the encrypted (N+1)-th layer data.

48. The method of claim 32, further comprising:
storing the encrypted (N+1)-th layer data; and
transmitting the encrypted and the stored (N+1)-th layer data upon a request from a user.

49. A method of hierarchically decrypting media data, the method comprising:
generating an N-th layer key;
generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;
decrypting encrypted N-th layer data using the N-th layer key; and
decrypting encrypted (N+1)-th layer data using the (N+1)-th layer key.

50. The method of claim 49, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

51. The method of claim 49, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

52. The method of claim 51, wherein the generating of the N-th layer key comprises:
receiving an N-th layer key and generating the N-th layer key.

53. The method of claim 51, wherein the generating of the N-th layer key comprises:
receiving an encrypted N-th layer key; and
decrypting the encrypted N-th layer key to generate the N-th layer key.

54. The method of claim 49, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

55. The method of claim 54, wherein the generating of the N-th layer key comprises:
generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

56. The method of claim 49, further comprising:
temporarily storing the N-th layer key;
commanding that the N-th layer key be generated according to meta-data when the meta-data is received; and
commanding that the stored N-th layer key be supplied to the decryption of the encrypted N-th layer data according to the meta data when the encrypted N-th layer data is received.

57. The method of claim 49, further comprising:
temporarily storing the (N+1)-th layer key;

commanding that the (N+1)-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored (N+1)-th layer key be supplied to the encryption of the (N+1)-th layer data according to the meta data when the encrypted (N+1)-th layer data is received.

58. A method of hierarchically encrypting and decrypting media data, the method comprising:

generating an N-th layer key;

generating an (N+1)-th layer key by applying the generated N-th layer key to a predetermined function;

encrypting N-th layer data using the N-th layer key, and encrypting (N+1)-th layer data using the generated (N+1)-th layer key;

generating the N-th layer key;

generating the (N+1)-th layer key by applying the N-th layer key to the predetermined function;

decrypting the encrypted N-th layer data using the N-th layer key; and

decrypting the encrypted (N+1)-th layer data using the (N+1)-th layer key.

59. The method of claim 58, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

60. The method of claim 58, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

61. The method of claim 58, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

62. The method of claim 61, further comprising:

generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

63. A computer readable storage medium controlling a computer and comprising a process of

generating an N-th layer key;

generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;

encrypting N-th layer data using the N-th layer key; and

encrypting (N+1)-th layer data using the (N+1)-th layer key.

64. The computer readable storage medium of claim 63, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

65. The computer readable storage medium of claim 64, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

66. The computer readable storage medium of claim 63, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

67. The computer readable storage medium of claim 66, wherein the generating of the N-th layer key comprises generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

68. The computer readable storage medium of claim 63, further comprising:

temporarily storing the N-th layer key;

commanding that the N-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored N-th layer key be supplied to encrypt the N-th layer data according to the meta data when the N-th layer data is received.

69. The computer readable storage medium of claim 63, further comprising:

temporarily storing the (N+1)-th layer key;

commanding that the (N+1)-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored (N+1)-th layer key be supplied to encrypt the (N+1)-th layer data according to the meta data when the (N+1)-th layer data is received.

70. The computer readable storage medium of claim 63, further comprising:

encrypting the N-th layer key.

71. The computer readable storage medium of claim 71, further comprising:

transmitting the encrypted N-th layer key.

72. The computer readable storage medium of claim 70, further comprising:

storing the encrypted N-th layer key; and

transmitting the encrypted and stored N-th layer key upon a request from a user.

73. The computer readable storage medium of claim 63, further comprising:

encrypting the (N+1)-th layer key.

74. The computer readable storage medium of claim 73, further comprising:

transmitting the encrypted (N+1)-th layer key.

75. The computer readable storage medium of claim 73, further comprising:

storing the encrypted (N+1)-th layer key; and

transmitting the encrypted and stored (N+1)-th layer key upon a request from a user.

76. The computer readable storage medium of claim 63, further comprising:

transmitting the encrypted N-th layer data.

77. The computer readable storage medium of claim 63, further comprising:

storing the encrypted N-th layer data; and

transmitting the encrypted and stored N-th layer data at a user's request.

78. The computer readable storage medium of claim 63, further comprising:

transmitting the encrypted (N+1)-th layer data.

79. The computer readable storage medium of claim 63, further comprising:

storing the encrypted (N+1)-th layer data; and

transmitting the encrypted and the stored (N+1)-th layer data upon a request from a user.

80. A computer readable storage medium controlling a computer and comprising a process of hierarchically decrypting media data, comprising:

generating an N-th layer key;

generating an (N+1)-th layer key by applying the N-th layer key to a predetermined function;

decrypting encrypted N-th layer data using the N-th layer key; and

decrypting encrypted (N+1)-th layer data using the (N+1)-th layer key.

81. The computer readable storage medium of claim 80, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

82. The computer readable storage medium of claim 80, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

83. The computer readable storage medium of claim 82, wherein the generating of the N-th layer key comprises:

receiving an N-th layer key and generating the N-th layer key.

84. The computer readable storage medium of claim 83, wherein the generating of the N-th layer key comprises:

receiving an encrypted N-th layer key; and

decrypting the encrypted N-th layer key to generate the N-th layer key.

85. The computer readable storage medium of claim 80, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

86. The computer readable storage medium of claim 85, wherein the generating of the N-th layer key comprises:

generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.

87. The computer readable storage medium of claim 80, further comprising:

temporarily storing the N-th layer key;

commanding that the N-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored N-th layer key be supplied to the decryption of the encrypted N-th layer data according to the meta data when the encrypted N-th layer data is received.

88. The computer readable storage medium of claim 80, further comprising:

temporarily storing the (N+1)-th layer key;

commanding that the (N+1)-th layer key be generated according to meta-data when the meta-data is received; and

commanding that the stored (N+1)-th layer key be supplied to the encryption of the (N+1)-th layer data according to the meta data when the encrypted (N+1)-th layer data is received.

89. A computer readable storage medium controlling a computer and comprising a process of hierarchically encrypting and decrypting media data, comprising:

generating an N-th layer key;

generating an (N+1)-th layer key by applying the generated N-th layer key to a predetermined function;

encrypting N-th layer data using the N-th layer key, and encrypting (N+1)-th layer data using the generated (N+1)-th layer key;

generating the N-th layer key;

generating the (N+1)-th layer key by applying the N-th layer key to the predetermined function;

decrypting the encrypted N-th layer data using the N-th layer key; and

decrypting the encrypted (N+1)-th layer data using the (N+1)-th layer key.

90. The computer readable storage medium of claim 89, wherein the predetermined function is a one-way function by which a value of the function is found from an input value but the input value is not found from the value of the function.

91. The computer readable storage medium of claim 89, wherein the N-th layer data is the entire media data except key clip data and key frame data, and the (N+1)-th layer data is the key clip data except the key frame data.

92. The computer readable storage medium of claim 89, wherein the N-th layer data is key clip data of the media data except key frame data of the media data, and the (N+1)-th layer data is the key frame data of the media data.

93. The computer readable storage medium of claim 92, further comprising:

generating the N-th layer key by applying an (N-1)-th layer key to the predetermined function.